
UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon. Lois H. Goodman
:
v. : Mag. No. 20-5036
:
ANDREW RAMEY : CRIMINAL COMPLAINT

I, Brian Teague, being duly sworn, state that the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

s/ Brian Teague

Brian Teague, Special Agent
Department of Homeland Security
Homeland Security Investigations

Attested to me by telephone,
pursuant to FRCP 4.1(b)(2)(A)

November 13, 2020,
in the District of New Jersey,



HONORABLE LOIS H. GOODMAN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

COUNT ONE

(Distribution of Child Pornography)

From on or about March 13, 2020, through June 8, 2020, in Ocean County, in the District of New Jersey, and elsewhere, the defendant,

ANDREW RAMEY,

did knowingly distribute material containing child pornography, as defined in Title 18, United States Code, Section 2256(8)(A), using any means or facility of interstate or foreign commerce or that had been mailed, or had been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

In violation of Title 18, United States Code, Section 2252A(a)(2)(B) and Title 18, United States Code, Section 2.

COUNT TWO
(Possession of Child Pornography)

On or about November 13, 2020, in Ocean County, in the District of New Jersey, and elsewhere, the defendant,

ANDREW RAMEY,

did knowingly possess material that contained images of child pornography, as defined in Title 18, United States Code, Section 2256(8), which had been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that had been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

In violation of Title 18, United States Code, Section 2252A(a)(5)(B).

ATTACHMENT B

I, Brian Teague, am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”). I have participated in this investigation, discussed this matter with other law enforcement officers, and have reviewed documents and other materials. Accordingly, I have personal knowledge of the facts set forth below. Because this criminal complaint is being submitted only for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this complaint are related in sum and substance and in part, and all dates and figures are approximate.

1. On or about November 29, 2018, defendant ANDREW B. RAMEY (“ANDREW RAMEY” or “RAMEY”), was convicted in the United States District Court for the District of New Jersey of possession of child pornography in violation of Title 18, United States Code, Section 2252A(a)(5)(B), and he was sentenced to 12 months’ imprisonment and 9 years’ supervised release. Defendant RAMEY was released from the custody of the Bureau of Prisons and commenced his term of federal supervised release on or about December 9, 2019. As a condition of his supervised release, defendant was required to reside at a residence in Brick Township, New Jersey (the “Residence”), and was subject to location monitoring. At all times relevant to this complaint, defendant RAMEY resided at the Residence.

2. As set forth below, within months of being released from prison, defendant RAMEY committed new child pornography offenses using, among other things, the BitTorrent Network.

3. The BitTorrent Network is a publicly available online peer-to-peer (“P2P”) file-sharing network, that is, a worldwide network of linked computers. To access the BitTorrent Network, a user must first download P2P software (“BitTorrent Software”), which is widely available for free on the Internet from numerous different companies and application designers. BitTorrent Software allows the user to, among other things, (1) place files into a designated “shared” folder on his or her hard drive, from which other BitTorrent users can then download those files directly to the “shared” folders of their own computers; and (2) search, select, and directly download, into his or her “shared” folder, files from the “shared” folders of other BitTorrent users. BitTorrent Software typically keeps a log of each download event, and forensic examiners can often determine, using such logs, from which Internet Protocol (“IP”) address a user obtained a particular file. Internet Service Providers (“ISPs”) assign a unique IP address to each computer or device that accesses the internet and typically keep records of the ISP customer accounts associated with each assigned IP address.

4. From on or about March 13, 2020, through on or about June 8, 2020 (collectively, the “Relevant Period”), law enforcement used BitTorrent Software to access the BitTorrent Network and, downloaded twelve (12) unique video and image files containing images of child sexual abuse and child pornography from a certain IP address (the “Target IP Address”). The files were downloaded from a shared folder on a device or devices assigned the Target IP Address.

5. HSI Special Agents have reviewed the video files downloaded from the device that was assigned the Target IP Address and identified them as containing images of child sexual abuse and child pornography. The following files, identified by their SHA hash values,¹ are a representative sample of the files that HSI Agents reviewed:

Filename and SHA Hash Value	Description
Filename: pthc pedo rare deepthroat 5yo wow no gaging.mpg SHA Hash Value: ANYLSKZQYRWKRC3Z6LAJOGCZDNXEC24Y	This video depicts a prepubescent female performing oral sex on an adult male. The female appears to be approximately 4-5 years old. The video is approximately 2 minutes and 19 seconds long.
Filename: PTCH 2014 (5yo GREAT ANAL).wmv SHA Hash Value: YCHIL4XZBZGWYHAHUYZCWKPB4DP4XMRR	This video depicts a prepubescent female, naked from the waist down, being penetrated by an adult male’s penis. The female appears to be approximately 5-6 years old. The video is 1 minute and 22 seconds long.

¹ The Secure Hash Algorithm (“SHA”) is a means of identifying files using a digital “fingerprint” that consists of a unique series of letters and numbers.

Filename: [julyjailbait.club] – russian boy fake fuck preteen sister (pthc, amateur).mp4 SHA Hash Value: EKKD342MLY3GFDS5MWTIAT7CL672OO7F	This video depicts a naked teenage boy, removing the pants of a prepubescent female before performing oral sex on the female’s vagina and penetrating the female’s vagina with his penis. The female appears to be approximately 8-10 years old. The video is 4 minutes and 45 seconds long.
---	--

6. Following some of law enforcement’s downloads during the Relevant Period as described above, HSI obtained ISP records indicating that the Target IP Address had been assigned to an ISP account (the “Account”) subscribed to the Residence. HSI also obtained IP address logs indicating that the Target IP Address had been assigned to the Account during the Relevant Period.

7. Based on its investigation, on or about November 13, 2020, law enforcement obtained and executed a search warrant at the Residence. During the search, law enforcement discovered and seized, among other things, an Android smartphone belonging to defendant RAMEY (the “Device”). Law enforcement located the Device in Defendant RAMEY’s living area within the Residence and, after being advised of his Miranda rights, defendant RAMEY provided the password to the Device. Law enforcement’s preliminary examination of the Device conducted at the Residence revealed that it contained BitTorrent Software and hundreds of images and more than ten videos depicting child pornography.² The images and videos depict, among other things, prepubescent children engaged in sexual acts with adults.

8. One of the video files that law enforcement found on the Device, with file name “pthc pedo rare deepthroat 5yo wow no gaging.mpg,” was the same child pornography file that law enforcement downloaded from a device using the Target IP Address during the Relevant Period, as confirmed by its unique SHA hash value.

² The Device contains thousands of image and video files, which HSI Special Agents are still in the process of reviewing as of the date of this criminal complaint.

9. Based upon my education, training and experience, and my discussions with other law enforcement officers, and to the best of my knowledge and belief, the images and videos described above were transported and transmitted in interstate commerce and were transported and transmitted using any means and facility of interstate and foreign commerce, including by computer, based upon, among other things, the presence of images and videos in the downloads folder of RAMEY's smartphone and the presence of BitTorrent Software on RAMEY's smartphone.

10. In addition, based upon my education, training and experience, and my discussions with other law enforcement officers, and to the best of my knowledge, the images and videos described above were produced using materials that were mailed, shipped, and transported in or affecting interstate or foreign commerce by any means, including by computer.